PCT

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)
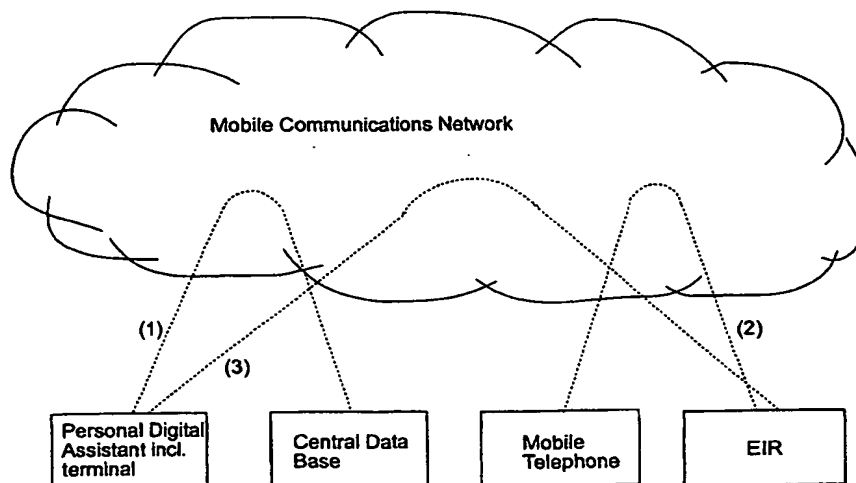
(51) International Patent Classification 7 : G06F 1/00, H04Q 7/38	A1	(11) International Publication Number: **WO 00/45243**
		(43) International Publication Date: 3 August 2000 (03.08.00)

(54) Title: PROTECTION AGAINST THEFT FOR PERSONAL DIGITAL ASSISTANT

(57) Abstract

A Personal Digital Assistant is a portable computer that is so small that it can be held in the hand at use. Such Personal Digital Assistants will be extensively used both for data processing and registration, and by that data will be stored in the Personal Digital Assistant. In order to handle registered data, Personal Digital Assistants normally include functionality for setup to central computer via mobile telecommunications network. The present invention relates to a protection against theft of information from Personal Digital Assistants that have integrated functionality for mobile telecommunication. The Personal Digital Assistant is so adapted that it is not possible to activate without it connecting itself to the mobile telecommunications network. If the terminal is stolen and reported to central register for protection against theft, the terminal can lock itself against access to data, change to a state where it is unusable, and delete stored information according to specification. By that, the stored information will be inaccessible, even if the whole Personal Digital Assistant falls into wrong hands.

TITLE OF THE INVENTION

Protection against theft for Personal Digital Assistant

5

TECHNICAL FIELD

A Personal Digital Assistant is a portable computer that is
so small that it can be held in the hand at use. Personal
10   Digital Assistants will be of extensive use both for data
processing and registration and by that data will be stored
in the Personal Digital Assistant or terminal. In order to
protect these stored data against unauthorised access, the
Personal Digital Assistant/terminal must be prepared in
15   such a way that the risk of theft of the Personal Digital
Assistant is limited.

The present invention relates to a system and a method to
protect stored data if the computer yet would fall into
20   wrong hands. The method and the system are applicable to
Personal Digital Assistants/terminals that are equipped
with terminal function for mobile communication. In the
first place the invention deals with a terminal that is
connected to a mobile packet switching data service such as
25   GPRS.

PRIOR ART

30   At a performed patent situation investigation, the
following documents have been found:

      D1.   JP,A,   8-272 742
      D2.   JP,A,   8-251 660
35   D3.   JP,A,   7-193 865
      D4.   JP,A,   9-322 246

D5. JP,A,   8-317 467
D6. US,A,   5 600 708
D7. US,A,   5 659 594

5   The documents D2-D7 describes systems and devices the main aim of which are to prevent that a stolen mobile terminal is used, in order to in that way protect the rightful owner from costs caused by utilisation of the mobile terminal.

10   In documents D2 and D3 ways are described to protect use of a lost or stolen portable terminal, by that the owner, at detection of that the terminal is lost or stolen, can utilise the public telephone network and from a terminal initiate transmission of a signal to the lost terminal. The
15   terminal that receives the signal will at that delete certain internal information, such as subscription information, which is important for the use of the terminal in the telecommunications network. By that is prevented that the stolen terminal can be used by unauthorised
20   person.

Documents D4, D6 and D7 describes portable terminals, which are adapted with automatic procedures for check of that use is allowed by a check of a code or a list, which is
25   transmitted from each base station. The terminal changes to the state "out of operation" if the code or list indicates that use is not allowed, for instance by checking of the IMEI-code.

30   There also are examples (document D5) of that a database is adapted to indicate the position of a lost portable terminal, which is in state of operation for use. If the terminal is stolen, use of the terminal also can be protected by breaking the setup in the mobile network.
35

Only one of the found documents, D1, describes a solution
that is intended to protect a mobile terminal against
disclosure of stored data. A portable terminal is adapted
in a way that the owner, at detection that the terminal is
5   lost or stolen, can utilise the public telephone network
and from a telephone initiate encryption of stored
information. When the encryption is finished, the
information that has been stored in the terminal to perform
the encryption is deleted.

10

None of the documents that have been found at the
investigation includes explicitly, or in combination, the
solution that is described in the present patent
application.

15

TECHNICAL PROBLEM

A Personal Digital Assistant, which is utilised to register
20   data will store great amounts of information. Among the
stored information there may be both recently registered
information and information that has been registered
earlier, but has not yet been deleted, as well as basic
data to facilitate the registration, application programs
25   and other software. The Personal Digital Assistant
therefore can hold information that are on different levels
of secrecy and which it for different reasons is important
to keep secret. In the Personal Digital Assistant built-in
locks, such as keyboard locks and screen savers or
30   mechanical access protection devices give a limited
protection, but such locks can be broken/forced and in many
cases there is a need for a more efficient protection
against unauthorised access to stored data. This is
especially important in connection with portable computers
35   and Personal Digital Assistants, since the possibilities to
disclose stored information are great because the computer

can be carried away and be thoroughly examined and also
dismantled.

At business activity, information is registered that
5   concerns the activity. The information can relate to i.a.
size of stock, assortment of articles and price
information, which information shall not be disclosed to
competitors. Information also can relate to parts of, or
basic data for offers, in which case neither the customer
10   under any circumstances at all shall have access to the
information.

At physician's round in hospital, previously registered
information about patients is stored, such as identity
15   information (for instance civic registration number),
information about previous diseases, medicines to be taken,
diagnosis and measured values. At the round, further
information can be added. It is of outmost importance that
such information is not accessible to unauthorised persons,
20   primarily with regard to the patient's interests, but also
in order to maintain the reputation of the care provider
and to fulfil law requirements.

If information about an operators operation activities is
25   made public, so that competitors will get information
about, for instance, total capacity or at present available
capacity, the current price situation can be influenced by
the competition advantages that one of the parties can get
by knowing information important for the operation. This is
30   made especially evident in a firm of brokers or in exchange
transactions, where often big business transactions are
performed within a short period of time, and with current
data as basic data information.

The user can use the Personal Digital Assistant as meeting calendar and take down meeting notes or make private or work related notes of delicate kind.

5   In addition to these examples Personal Digital Assistants will be used in a lot of other applications.

If an unauthorised person gets hold of the Personal Digital Assistant, one therefore will risk a great deal of harm if
10   the Personal Digital Assistant is not adapted so that it is possible to prevent that the stored information is disclosed. A lock of type keyboard lock/window lock, or a mechanical lock, gives a limited protection against disclosure. A more efficient protection is achieved if
15   stored data cannot be interpreted to usable information. To attain this there are two possibilities:

- Efficient encryption of stored information, completed with a good protection by means that causes decryption
20   or other interpretation of the information.

- Deletion of stored information, the disclosure of which to unauthorised person results in harm.

25   One solution with utilisation of the first of the above mentioned possibilities is described above under "Prior Art", said document D1.

The invention according to the present patent application
30   solves the problem of protecting the information according to the second of the two possibilities above.

35

TECHNICAL SOLUTION

A packet switching data service such as GPRS offers
improved possibilities to create a protection for data
5   stored in Personal Digital Assistants, which are equipped
with terminal function for mobile communication.

A Personal Digital Assistant, which is equipped with
integrated function for mobile communication, can be
10   adapted so that it will not be possible to activate without
it connecting itself to the mobile telecommunications
network. If the terminal is stolen and reported to central
register for protection against theft (EIR - Equipment
Identification Register), the terminal can lock itself
15   against access of data, change into a state where it is
unusable, and delete certain stored information. By that,
the stored information will be inaccessible, even if the
whole Personal Digital Assistant will fall into wrong
hands.
20
The Personal Digital Assistant in addition to that can be
adapted so that register check via EIR is a condition for
access to certain data. In the same way the information of
the Personal Digital Assistant then will be protected if
25   the terminal turns out to be reported as stolen.

ADVANTAGES

30   If the user has lost the Personal Digital Assistant and
suspects that it has got into wrong hands, he/she can in a
simple way initiate protection of the stored information.
Immediately when the Personal Digital Assistant is
activated, an automatic process will check whether the
35   Personal Digital Assistant is registered as stolen. If this
is the case, certain specified information will be deleted

and the Personal Digital Assistant is set in a state where
it is unusable, before the user has possibility to interact
with the Personal Digital Assistant. In that way, the
information will have an efficient protection against
disclosure. At the deletion, registered data that have not
yet been transferred to central storing are lost. The
amount of data that can be lost at deletion can be limited
by data frequently being transferred to central storing, to
avoid that backup has not been taken for large amounts of
data. This is also important in order to protect registered
data against loss caused by technical errors in the
Personal Digital Assistant, or by disturbances/
interruptions.

In connection with deletion of data there is also
possibility to delete stored programs and other routines so
that misuse of licences (program copying) can be avoided.

If the program supplier has especially large demands of
protection on the software, demands can be called for that
the software is well protected against disclosure. In such
cases the present invention gives a possibility to use
programs, which otherwise are not allowed to be used in
Personal Digital Assistants or other portable computers.

At the same time as the information protection is executed,
the Personal Digital Assistant is set in a state making it
considerable less usable, i.a. by that misuse of services
that are connected to the Personal Digital Assistant, for
instance services subscribed to in telecommunications
networks, can be prevented. By that, the value for
unauthorised use is reduced, resulting in that the Personal
Digital Assistant at the same time becomes less liable to
be stolen.

DESCRIPTION OF DRAWINGS

Figure 1 shows a block diagram for the communication
procedure at activation of the Personal Digital Assistant.

Figure 2 shows activation of Personal Digital Assistant and
activities in the Personal Digital Assistant in connection
with blocking.

EXPLANATIONS OF TERMS

EIR   Equipment Identification Register.
            Register, for protection against theft, that
            stores serial numbers (IMEI) of stolen
            communication equipment for mobile telephony. By
            using the register, blocking of stolen equipment
            is made possible.

IMEI   International Mobile Equipment Identity.
            International serial number for communication
            equipment for mobile telephony. Each such
            communication equipment is by that uniquely
            identified.

GPRS   Generalised Packet Radio Service.
            Packet switching data service for GSM.

GSM   Global System for Mobile communication.

PDA   Personal Digital Assistant.
            Portable computer that is so small that it can be
            held in the hand at use.

DETAILED DESCRIPTION

The description below refers to the figures in the enclosed drawings.

5

THE PERSONAL DIGITAL ASSISTANT

Personal Digital Assistants are used in many different
10   connections, such as by service and selling staff, in the transport sector, the industry and the retail trade. Common applications are reception and dispatching of goods, stock-taking and collecting according to orders. The Personal Digital Assistant also can include the user´s meeting
15   calendar and meeting notes, as well as private or work related notes of delicate kind. Use of Personal Digital Assistants will be improved and they will be used in new fields. Example of possible new fields are within care/nursing, which make new demands on protection of the
20   information.

With the Personal Digital Assistant, access to data will be faster, and the information that is registered will be more accurate than by use of conventional registration. Use of
25   Personal Digital Assistant therefore will be both time and cost saving. The software for the Personal Digital Assistant can be tailored, but there are also standard programs for more simple routines.

30   At use of the Personal Digital Assistant, stored data about the object that are to be dealt with are used. Data is fed into and stored in the Personal Digital Assistant for later processing or storing in central systems. Transfer of data to central systems can be made by transmission via mobile
35   telephony, which this invention is dealing with.

EQUIPMENT IDENTIFICATION REGISTER

A register for protection against theft, for instance EIR,
over terminals for mobile telecommunication is managed by a
5   trusted organisation.

The register includes a list over reported stolen/lost
terminals that shall be protected against unauthorised use.
Reported terminals are identified by the serial number
10   IMEI.

THE IDEA OF THE INVENTION

15   The invention relates to a portable computer, which
includes functionality for setup to central computer via
mobile telecommunications network. The connection to the
central computer is utilised, for instance, for transfer of
data, which have been registered in the Personal Digital
20   Assistant, or for reception of data or other information
from the central computer. At connection to the
telecommunications network, check (23) is made in register
for protection against theft, whether the mobile telephone
has been reported as stolen. If that is not the case,
25   connection is made to the network, and the computer is
started in normal operation.

The computer is so adapted that it in connection with
activation (21) connects itself to the mobile
30   telecommunications network (22) in a procedure that cannot
be cut off/interrupted. In order to prevent unauthorised
use of the Personal Digital Assistant, before the
protection against theft comes into effect, the connection
to the mobile telecommunications network is made before
35   security protected functions and data in the Personal
Digital Assistant are made accessible to the user. This

can, for instance, be achieved by the man-machine interface
in the Personal Digital Assistant not being activated
before the connection to the mobile telecommunications
network is performed.

5

If the computer is stolen, or lost in another way, the loss
is reported to the register for protection against theft by
report of the identity of the terminal, for instance by
report of IMEI, at which the terminal will be protected
10   against use in the mobile telecommunications network.

The function "protection against theft" in the mobile
telephone network means that if said check shows that a
terminal, which requests connection to the
15   telecommunications network, has been registered as stolen,
the connection will not be made. The terminal also will be
blocked.

In that way, a mobile telephone/Personal Digital Assistant,
20   which has been registered as stolen, will, according to the
invention, be prevented to connect itself to the mobile
telecommunications network. At that, the terminal will
change to protected state. This means that such data that
have been stored in the Personal Digital Assistant and
25   which have been judged to need secrecy protection, are
deleted (24). The scope of the protection against theft is
selected so that it corresponds to the needs, depending on
the design of the computer and the need of protection for
data that are handled. In certain applications of the
30   Personal Digital Assistant, only fed in data are deleted,
whereas in other applications also stored basic data,
databases, programs and control sequences etc, are deleted.
Encryption of certain, or all, data can be an alternative,
or complement, to deletion of data.

35

In order to get a better continuity of the supervision
against theft, check (23) in register for protection
against theft whether the mobile telephone has been
reported as stolen, also can be made on other occasions

5   than at activation of the computer, for instance in
connection with data transmission on the network, or after
a stipulated period of time. Check (23) in register for
protection against theft can also be initiated in
connection with file access. At one in that way certified

10   theft report, the Personal Digital Assistant will, in a
corresponding way, be protected by i.a. deletion of stored
data and blocking, as well as prevention, of transmission
of data via the telecommunications network.

15   Performed deletion may be signalled over the mobile
telecommunications network to instance with a supervising
function for the Personal Digital Assistant. Such a
supervising instance can be above mentioned central
computer, or an alarm centre. After deletion, the computer

20   changes to blocked state (25). Connection to the
telecommunications network can be maintained as long as the
computer is on, in order to facilitate localisation as a
means to find the computer again.

25   In below described embodiments, the description is based on
use of the packet switching data network GPRS.
Alternatively other packet switching telecommunications
networks can be utilised. The invention also can, under
certain circumstances, be utilised at telecommunications

30   networks without packet data switching.

PREFERRED EMBODIMENT

35   A Personal Digital Assistant intended to be used in a
mobile way, for instance to register information such as

stocktaking, is equipped with an integrated GPRS-terminal. The computer is loaded with programs and data files necessary for the registration activity and has storing space for the data that shall be registered. The computer

5   also has been equipped with functions for handling of the GPRS-terminal and functions for protection of stored data. The memory areas that will hold information that shall be protected against disclosure, shall be specified. If the functions for protection of stored data are activated,

10 these specified data areas then will be protected against disclosure by deletion.

When the computer is activated, a connection to the GSM-network is made by a GPRS attach, and the GPRS-terminal

15 will get into the state READY. In the GSM-network is checked whether the terminal/computer is registered as stolen by check of the IMEI of the terminal in EIR. If the terminal/Personal Digital Assistant is not reported as stolen, GPRS attach is performed and the GPRS-terminal will

20 be accessible. After that, the terminal/Personal Digital Assistant is activated and an be used in intended way.

If the terminal/Personal Digital Assistant turns out to be reported as stolen, the Personal Digital Assistant will,

25 via the GPRS-terminal, have a message to change to blocked state. At that, all man-machine communication will be blocked, and specified data areas will be deleted. At the same time connection to the GSM-network will be blocked, to prevent the GPRS-terminal from being used. This means that

30 it is not possible to read data from the terminal, neither via keyboard and screen, nor via the GPRS-service. Because the data areas are deleted, where secret information can have been stored, all delicate data will be inaccessible, even if the Personal Digital Assistant is demounted.

35

ALTERNATIVE EMBODIMENTS

Some computers are located to environments and situations
where it is difficult to create a satisfactory protection
5   against theft. Examples of such situations are portable
computers and computers located at public places or fairs.
A computer that is expected to be subject to a bigger risk
to be stolen is equipped with an integrated GPRS-terminal.

10   The computer is loaded with programs and data files
necessary for the activity, and has storing capacity for
data that shall be registered. Depending on demands of
secrecy, the computer can be equipped with storing space
that allows efficient deletion of memory content. The
15   computer in addition has been equipped with functions for
handling of the GPRS-terminal, and functions for protection
of stored data.

When the computer is activated, an automatic connection is
20   made to the GSM-network, and a check whether the
terminal/computer is reported as stolen. If the terminal/
computer turns out to be registered as stolen, the computer
will, via GPRS, have a message to protect stored data and
change to blocked state. Depending on the situation,
25   different degrees of protection can be applied. The man-
machine communication can be cut off, and selected memory
areas can be deleted.

By means of a time supervision, the GPRS-terminal can
30   detach, and immediately after that attach. An
activated/switched on computer can in that way get an
efficient protection against theft of data.

The same protection can be achieved by utilisation of other
35   packet data switching telecommunication networks than GPRS,
for instance UMTS.

By utilising text messages, the secrecy protection can work also in mobile telecommunications networks without packet data switching.

5

The invention is not limited to the above described embodiments, but may also be subject to modifications within the frame of the following patent claims and the idea of invention.

PATENT CLAIMS

1. A method for protection against theft of information
    that has been stored in portable computer with
    integrated terminal for mobile telecommunication,
    c h a r a c t e r i s e d in, that at connection to
    telecommunications network, check (23) is made in
    register for protection against theft whether said
    terminal, which is integrated in said computer, has
    been reported as stolen.

2. A method, as claimed in patent claim 1,
    c h a r a c t e r i s e d in, that said portable
    computer is adapted in a way that it, in connection
    with activation (21), connects itself to
    telecommunications network (22) for mobile
    telecommunication, before security protected functions
    and data, which have been stored in said computer, are
    made accessible to the user.

3. A method, as claimed in patent claim 1 or 2,
    c h a r a c t e r i s e d in, that if said check shows
    that said terminal, which requests connection to the
    telecommunications network, has been registered as
    stolen, the connection is not made.

4. A method, as claimed in any of the previous patent
    claims, c h a r a c t e r i s e d in, that the
    procedure for said connection to telecommunications
    network (22) cannot be interrupted/cut off without the
    computer becoming deactivated.

5. A method, as claimed in any of the previous patent
    claims, c h a r a c t e r i s e d in, that said check
    (23) in register for protection against theft can be
    initiated in connection with:

•   file access,

•   data transmission on the network,

•   after a defined period of time, or

•   according to any other criterion.

6. A method, as claimed in any of the previous patent claims, c h a r a c t e r i s e d in, that the terminal will be registered as stolen in the register for protection against theft when the person, who has at his/her disposal said computer with integrated terminal, no longer is possessed of the computer, for instance if the computer has been stolen.

7. A method as claimed in any of the previous patent claims, c h a r a c t e r i s e d in, that connection to said register for protection against theft is made by registration of the serial number of the terminal, for instance IMEI, and in that said register for protection against theft is EIR (Equipment Identification Register).

8. A method as claimed in any of the previous patent claims, c h a r a c t e r i s e d in, that if said check in register for protection against theft shows that said terminal has been registered as stolen,

•   specified memory areas in the computer are deleted,

•   use of the computer is blocked;

•   the terminal function of the computer in the telecommunicationsnetwork is blocked.

9.   A method as claimed in any of the previous patent
claims, c h a r a c t e r i s e d in, that said specified
memory areas hold, or can hold, data or programs the
disclosure of which to unauthorised person can be harmful
5   to the owner of the computer.

10.   A method as claimed in any of the previous patent
claims, c h a r a c t e r i s e d in, that said portable
computer is a Personal Digital Assistant.

10

11.   A method as claimed in any of the previous patent
claims, c h a r a c t e r i s e d in, that packet switching
data service in the telecommunications network is utilised
by said integrated terminal for mobile telecommunication.

15

12.   A method as claimed in any of the previous patent
claims, c h a r a c t e r i s e d in, that said packet
switching data service is GPRS.

20   13.   A system for protection against theft of information
that has been stored in a portable computer, which has
integrated terminal, c h a r a c t e r i s e d in,

•   that said portable computer is adapted in a way that
25   it in connection with activation (21) connects itself
to telecommunications network (22) for mobile
telecommunication, before security protected functions
and data in the Personal Digital Assistant are made
accessible to the user, or the man-machine interface
30   in the computer is activated, and

•   that, at connection to the telecommunications network,
check (23) is made in register for protection against
theft if said terminal, which is integrated in said
35   computer, has been reported as stolen, and

-     that, if said terminal has been reported as stolen, communication on the telecommunications network is not accessible to the user.

14. A system as claimed in patent claim 13, c h a r a c t e r i s e d in, that the procedure for said connection to telecommunications network (22) cannot be interrupted/cut off without the portable computer becoming deactivated.

15. A system as claimed in any of the patent claims 13, or 14, c h a r a c t e r i s e d in that said check (23) in register for protection against theft can be initiated in connection with;

-     file access,

-     data transmission on the network,

-     after a specified period of time, or

-     according to another criterion.

16. A system as claimed in any of the patent claims 13 to 15, c h a r a c t e r i s e d in, that if said check in register for protection against theft shows that said terminal has been registered as stolen:

-     such memory areas that hold, or can hold, data or programs, the disclosure of which to an unauthorised person may result in harm to the owner of said computer, are deleted;

-     use of the computer is blocked, and

- the terminal function of the computer in the
  telecommunications network is blocked.

17. A system as claimed in any of the patent claims 13 to
5   16, c h a r a c t e r i s e d in, that said portable
     computer is a Personal Digital Assistant.

18. A system as claimed in any of the patent claims 13 to
     17, c h a r a c t e r i s e d in, that packet switching
10   data service in the telecommunications network is utilised
     by said terminal for mobile telecommunication, and in that
     said packet switching data service can be GPRS.

19. A system as claimed in any of the patent claims 13 to
15   18, c h a r a c t e r i s e d in, that said register for
     protection against theft is included in service for
     protection against theft, which is managed by trusted
     organisation, and in that connection and report regarding
     loss to said register for protection against theft is made
20   by registration of the serial number of the terminal.

20. A system as claimed in any of the patent claims 13 to
     19, c h a r a c t e r i s e d in, that the serial number of
     the terminal is IMEI, and said register for protection
25   against theft is EIR.

21. A system as claimed in any of the patent claims 13 to
     20, c h a r a c t e r i s e d in, that theft of the
     terminal is registered in the register for protection
30   against theft when the person who has at his/her disposal
     said portable terminal with integrated terminal, no longer
     is possessed of the computer, for instance if the computer
     has been stolen.

35   22. Use of EIR at a terminal, which is adapted to mobile
     telecommunication, and which is integrated in Personal

Digital Assistant, the memory areas of which hold, or can hold, data or programs, the disclosure of which to an unauthorised person may result in harm to the owner of the computer, by at theft, or other loss of said terminal

5   integrated in said Personal Digital Assistant, register the loss in order to, at activation of said Personal Digital Assistant but before security protected functions and data in the Personal Digital Assistant are made accessible to user, for instance by activation of the man-machine system,

10   via packet switching data service in mobile telecommunications network, check whether registration exists that said terminal has been lost or been stolen and, at verification of such registration, protect specified in said Personal Digital Assistant stored data or programs

15   against disclosure to unauthorised person by blocking connection of said terminal to the telecommunications network, delete specified memory areas in said Personal Digital Assistant, and block the use of the computer.
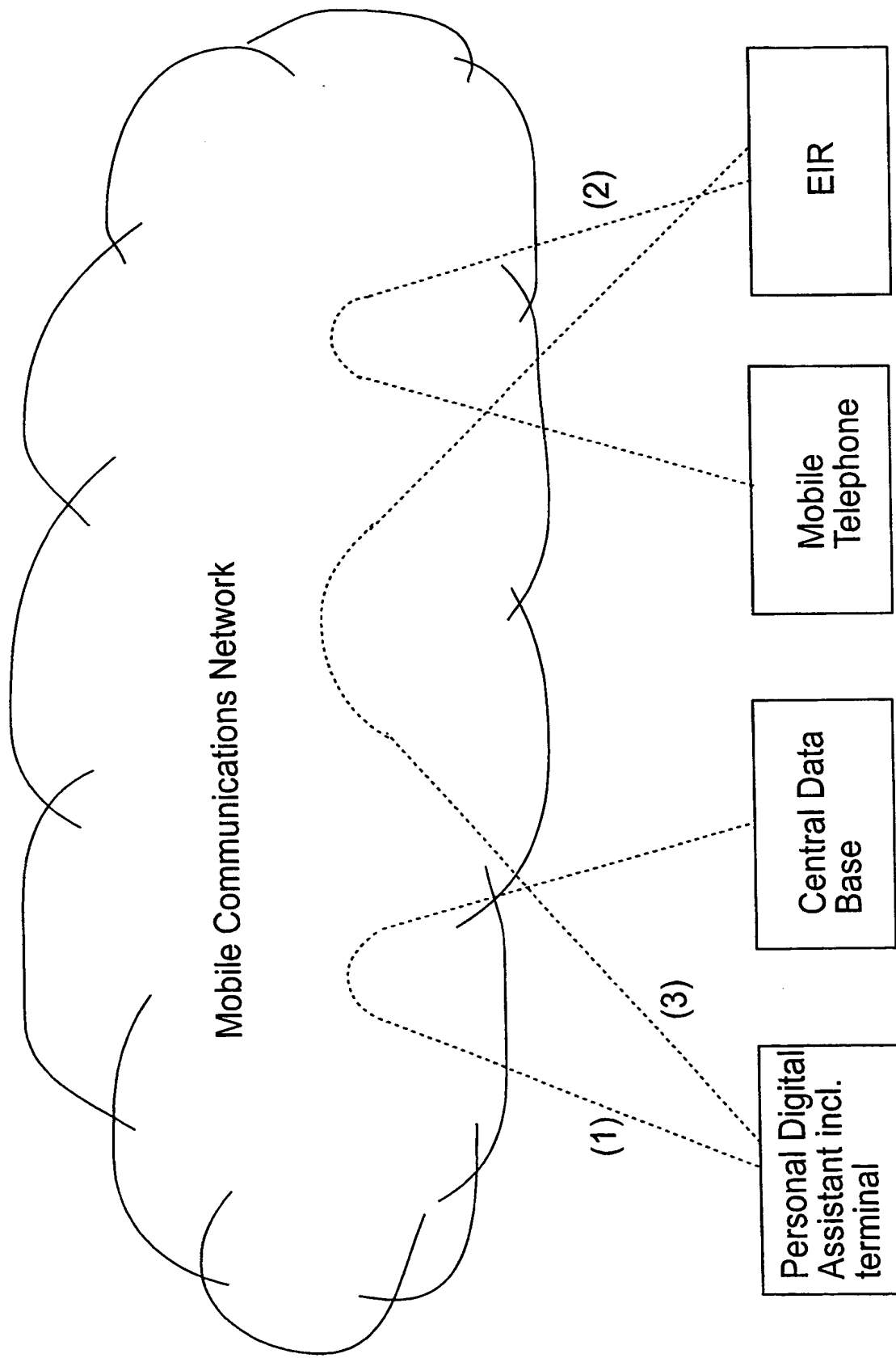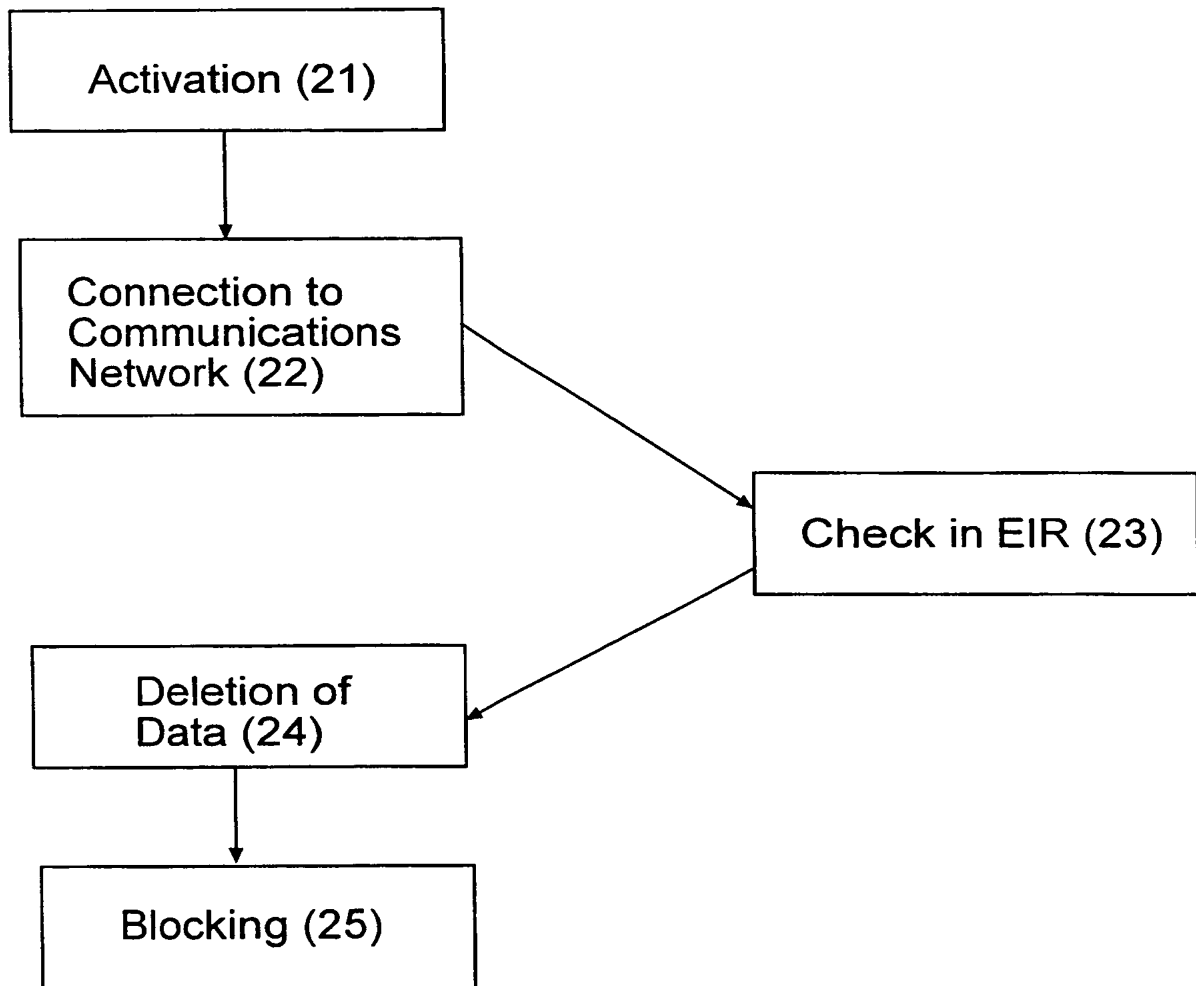
FIGURE 1

```
┌─────────────────────┐
│   Activation (21)   │
└─────────────────────┘
           │
           ▼
┌─────────────────────┐
│ Connection to       │
│ Communications      │─────────┐
│ Network (22)        │         │
└─────────────────────┘         │
                                ▼
                    ┌─────────────────────┐
                    │  Check in EIR (23)  │
                    └─────────────────────┘
┌─────────────────────┐         │
│ Deletion of         │◄────────┘
│ Data (24)           │
└─────────────────────┘
           │
           ▼
┌─────────────────────┐
│   Blocking (25)     │
└─────────────────────┘
```

FIGURE 2

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 1/00, H04Q 7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G06F, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5659595 A (FREDERIC CHANU ET AL), 19 August 1997 (19.08.97), column 1, line 11 - line 32, claims 1,2	1,3,5,6,7, 9-12
Y		8
A		2,4,13-22
	--	
Y	Patent Abstracts of Japan, abstract of JP 2-196532 A (MATSUSHITA ELECTRIC IND CO LTD), 3 August 1990 (03.08.90)	8
	--	

☐ Further documents are listed in the continuation of Box C.	☒ See patent family annex.

Date of the actual completion of the international search	Date of mailing of the international search report
22 June 2000	2 8 -06- 2000
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. + 46 8 666 02 86	Authorized officer Oskar Pihlgren/mj Telephone No. + 46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
US 5659595 A	19/08/97	AU	692831 B	18/06/98
		AU	1612495 A	05/10/95
		CA	2145600 A	30/09/95
		EP	0675659 A	04/10/95
		FI	951448 A	30/09/95
		FR	2718310 A,B	06/10/95
		JP	7274246 A	20/10/95
		NZ	270701 A	29/01/97

THIS PAGE BLANK (USPTO)